Paper No. 17

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte JAMES P. HUGHES

Appeal No. 2003-1942
Application No. 09/260,796

ON BRIEF

Before THOMAS, GROSS, and BARRY, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

A patent examiner rejected claims 1-5, 7, 9-11, 13, and 15-17. The appellant appeals therefrom under 35 U.S.C. § 134(a). We reverse.

BACKGROUND

The invention at issue on appeal stores and retrieves data securely. (Spec. at 1.) More specifically, the appellant seeks to limit access to data based on combinations of groups of clients. A group may be defined as clients sharing a common mandate, e.g., a financial department or a board of directors. (*Id.* at 10.)

Accordingly, the appellant uses an encryption value ("EV") to encrypt data before storing the data on an "untrusted" storage device. He then encrypts the EV; the EV is decrypted by solving an access formula describing a function of groups. Each group includes a list of at least one consumer client. A consumer client is granted access to the data if the client belongs to at least one group that solves the access formula. (*Id.* at 31.)

A further understanding of the invention can be achieved by reading the following claim.

> 3. A method for the secure handling of information by at least one client using at least one untrusted storage device, each client connected to the at least one untrusted storage device using a network, the network further having a key manager for issuing private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key, the method comprising:
>
> creating at least one group, each group comprising a list of at least one consumer client;
>
> acquiring a public key and a matched private key for each of the at least one group;
>
> encrypting an information set to produce a data set, the encryption based on a randomly generated number;
>
> determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group

indicating that a consumer client belonging to the at least one solution group may access the encrypted information set;

asymmetrically encrypting the randomly generated number using the determined access formula and the public key for each of the at least one group granted access to the information set;

adding the encrypted randomly generated number to the data set; and

storing the data set on at least one untrusted storage device.

Claims 1, 2, 9, 11, 13, and 15-17 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,787,175 ("Carter"). Claims 3-5, 7, and 10 stand rejected under 35 U.S.C. § 103(a) as obvious over Carter and U.S. Patent No. 3,798,360 ("Feistel").

OPINION

Our opinion addresses the claims in the following order:

- claims 1 and 2
- claims 3-5 and 7
- claims 9-11, 13 and 15-17.

A. CLAIMS 1 AND 2

Rather than reiterate the positions of the examiner or the appellant *in toto*, we focus on the point of contention therebetween. The examiner finds, "Carter elaborates

that the user inputs a user identifier and password; the member definitions of the collaborative document are searched in order to locate the member identifier corresponding to the user identifier." (Examiner's Answer at 13.) He then explains, "[i]n Carter, the client is a member of M-of-N groups, where both M and N equal one." (*Id.* at 16.) The appellant argues, "Carter does not contemplate basing access on a function, or on more than one group, or on a function of such groups." (Reply Br. at 4.)

In addressing the point of contention, the Board conducts a two-step analysis. First, we construe the claim at issue to determine its scope. Second, we determine whether the construed claim is anticipated.

1. Claim Construction

"Analysis begins with a key legal question — *what* is the invention *claimed*?" *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1567, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987). "[E]very limitation positively recited in a claim must be given effect in order to determine what subject matter that claim defines." *In re Wilder*, 429 F.2d 447, 450, 166 USPQ 545, 548 (CCPA 1970). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 1424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

Here, claim 1 recites in pertinent part the following limitations: "an access formula describing a function of groups, each group comprising a list of at least one client. . . ." As noted by the appellant, the claim "provides that the access formula describes a function of *groups*. Groups is [sic] plural." (Reply Br. at 4.) Accordingly, the limitations require an access formula describing a function of more than one group of clients.

2. Anticipation Determination

"Having construed the claim limitations at issue, we now compare the claims to the prior art to determine if the prior art anticipates those claims." *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349, 64 USPQ2d 1202, 1206 (Fed. Cir. 2002). "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (citing *Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707, 715, 223 USPQ 1264, 1270 (Fed. Cir. 1984); *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983); *Kalman v. Kimberly-Clark Corp.*, 713 F.2d760, 771, 218 USPQ 781, 789 (Fed. Cir. 1983)). "[A]bsence from the reference of any claimed

element negates anticipation." *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571, 230 USPQ 81, 84 (Fed. Cir. 1986).

Here, the examiner explains, "[i]n Carter, the client is a member of M-of-N groups, where both M and N equal one." (Examiner's Answer at 16.) As reasoned by the appellant, however, "if M=N=1, the access formula would be a function of only one *group*. Group is singular." (Reply Br. at 4.) In fact, the examiner admits, "Carter does not teach more complex formulas," (Examiner's Answer at 16); "Carter does not discuss values of M and N, each greater than one." (*Id.*) The absence of an access formula describing a function of more than one group of clients negates anticipation. Therefore, we reverse the anticipation rejection of claim 1 and of claim 2, which depends therefrom.

B. CLAIMS 3-5 AND 7

The examiner finds that "Carter depicts . . . encrypting the data portion of a document with a generated document key, preferably for use with a symmetric encryption method (see column 13, lines 4-17; figure 2, item 50 and 54; figure 3, items 68 and 70; figure 4, item 94; and figure 6, step 112); . . . encrypting the document key with the public key of the collaborative group (see column 13, lines 63-

67; column 14, lines 1-5 and figure 5, item 100). . . ." (Examiner's Answer at 7-8.) He further finds, "Feistel specifies a random key number generator in a symmetric key block cipher (see column 5, lines 18-23 and figure1, item 43)." (*Id.* at 8.) Noting that "[c]laim 3 also provides for encrypting an information set based on a randomly generated number and encrypting the randomly generated number using the access formula and the public key for each of the at least one group granted access to the information set," (Reply Br. at 8), the appellant argues, "[t]he Examiner points to no teaching or suggestion, in either Carter or Feistel, of such an encryption." (*Id.*)

In addressing the point of contention, the Board conducts a two-step analysis. First, we construe the claim at issue to determine its scope. Second, we determine whether the construed claim would have been obvious.

1. Claim Construction

Claim 3 recites in pertinent part the following limitations: "encrypting an information set to produce a data set, the encryption based on a randomly generated number; determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a consumer client belonging to the

at least one solution group may access the encrypted information set; asymmetrically encrypting the randomly generated number using the determined access formula and the public key for each of the at least one group granted access to the information set. . . ." Accordingly, the limitations require using a randomly generated number to encrypt information, determining an access formula expressing logical combination of at least one group for which access to the information will be granted, and using the determined access formula and a public key for the group granted access to the information to encrypt asymmetrically the randomly generated number.

2. Obviousness Determination

Having determined what subject matter is being claimed, the next inquiry is whether the subject matter would have been obvious. "In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "'A *prima facie* case of obviousness is established when the teachings from the prior art itself would . . . have suggested the claimed subject matter to a person of ordinary skill in the art.'" *In re Bell*, 991 F.2d 781, 783, 26 USPQ2d 1529,

1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

Here, Feistel discloses "a cryptographic coding process to maintain privacy of communications in a data processing network." Col. 1, ll. 52-54. The reference uses a randomly generated number to encrypt information. Specifically, "a random combination of binary digits is utilized to form the key for operating the cryptographic device that develops [a] first cipher block. Then, a portion of the first cipher block is stored and the remaining portion is combined with the same randomly generated binary digits to form a second ciphertext. The second ciphertext and the stored portion of the first cipher text are then combined to form a new composite cipher block that is transmitted." Col. 2, ll. 30-42. Furthermore, we agree with the examiner that "Carter's elaborat[ion] that the user inputs a user identifier and password; the member definitions of the collaborative document are searched in order to locate the member identifier corresponding to the user identifier," (Examiner's Answer at 13), constitutes an access formula expressing a logical combination of at least one group for which access to information will be granted.

The examiner does not allege, let alone show, that the teachings from Carter and Feistel would have suggested using the Carter's member definitions and public key for each group granted access to the information to encrypt asymmetrically Feistel's random combination of binary digits. Absent a teaching or suggestion of using an access formula and the public key for each group granted access to information to encrypt asymmetrically a randomly generated number, we are unpersuaded of a *prima facie* case of obviousness. Therefore, we reverse the obviousness rejection of claim 3 and of claims 4, 5, and 7, which depend therefrom.

C. CLAIMS 9-11, 13 AND 15-17

Citing "[c]olumn 8, lines 60-67," (Examiner's Answer at 17), and "[c]olumn 11, lines 55-67," (*id.*), the examiner asserts, "Carter teaches a group server obtaining a private key and matched public key for each group. . . ." (*Id.*) The appellant argues, "Carter teaches obtaining a public key and a private key only for each authorized *user*, not each group." (Reply Br. at 5.)

1. Claim Construction

Claim 9 recites in pertinent part the following limitations: "at least one group server connected to the network, each group server operable to (a) maintain at least

one group, each group comprising a list of client members allowed access to information produced by any client member of the group, and (b) obtain a private key and matched public key for each group. . . ." Accordingly, the limitations require obtaining a public key and a matched private key for a group comprising more than one client.

2. Anticipation and Obviousness Determinations

The first passage of Carter cited by the examiner discloses in pertinent part that an "operating system 46 generates, maintains, and manages a set of user identifiers 48 such as login names or account numbers." Col. 8, ll. 51-52. The second passage he cites discloses in pertinent part that "key pairs 76 are stored in key objects 74. In alternative embodiments, the key pairs 76 are stored in key attributes 74 which are then associated with user objects 68, with group objects 70, and/or with organizational role objects 72." Col. 11, ll. 61-65. We find no teaching in either passage of obtaining key pairs for a group. To the contrary, the reference obtains individual keys for users. Specifically, a "collaborative access controller 44 obtains one public key 78 for each collaborative group member." Col. 13, ll. 30-31.

The absence of obtaining a public key and a matched private key for a group of more than one client negates anticipation. Therefore, we reverse the anticipation rejection of claim 9 and of claims 11, 13 and 15-17, which depend therefrom.

The examiner does not allege, let alone show, that the addition of Feistel cures the aforementioned deficiency of Carter. Absent a teaching or suggestion of obtaining a public key and a matched private key for a group of clients, we are unpersuaded of a *prima facie* case of obviousness. Therefore, we reverse the obviousness rejection of claim 10.

CONCLUSION

In summary, the rejection of claims 1, 2, 9, 11, 13 and 15-17 under § 102(e) is reversed. The rejection of claims 3-5, 7, and 10 under § 103(a) is also reversed.

REVERSED

JAMES D. THOMAS)
Administrative Patent Judge)
)
)
ANITA PELLMAN GROSS) BOARD OF PATENT
Administrative Patent Judge) APPEALS
) AND
) INTERFERENCES
)
)
)
LANCE LEONARD BARRY)
Administrative Patent Judge)

TIMOTHY R. SCHULTE
STORAGE TECHNOLOGY CORPORATION
2270 SOUTH 88TH STREET MS-4309
LOUISVILLE, CO 800284309